We Claim:

1. A method for controlling the use of data on a device by a user, comprising the steps of:

issuing a smart card to the user by a first party, wherein a private key which is assigned to the user is stored on the smart card, wherein the private key is usable but not known by the user and the private key can not be used until the card is activated by authenticating that the user is authorized to use the smart card;

encrypting data to be sent to the user using a public key assigned to the user before distributing the data to the user; and

after distribution of the data to the user, prompting the user to enter a private key each time the user wants to use the data, wherein the user inserts the smart card into a smart card reader connected to the device and activates the smart card, wherein the device decrypts the encrypted data using the private key.

2. The method according to claim 1, wherein the smart card is a credit card.

3. The method according to claim 1, wherein the smart card is an identification card.

4. The method according to claim 1, wherein the data is digital information comprises one of computer software, music, literature, audio and/or video information.

5. The method according to claim 1, wherein the public and private keys are asymmetric public and private keys.

6. The method according to claim 5, wherein the asymmetric public key for the user is obtained from the user.

7. The method according to claim 5, wherein the asymmetric public key for the user is obtained from a public database.

8. The method according to claim 1, wherein the user authenticates the smart card by entering a personal identification number code.

9. The method according to claim 1, wherein the user authenticates the smart card by entering a biometric identification code.

10. The method according to claim 1, wherein a processor in the smart card decrypts the encrypted data using the private key.

11. A method for controlling the use of data on a device by a user, comprising the steps of:

issuing a smart card to the user by a first party, wherein a first private key which is assigned to the user is stored on the smart card, wherein the first private key is usable

but not known by the user and the first private key can not be used until the card is activated by authenticating that the user is authorized to use the smart card;

obtaining at least a second set of public and private keys and storing the at least second private key on the smart card;

encrypting data to be sent to the user using a first public key assigned to the user and the second public key before distributing the data to the user; and

after distribution of the data to the user, prompting the user to enter the first and at least second private keys each time the user wants to use the data, wherein the user inserts the smart card into a smart card reader connected to the device and activates the smart card, wherein the device decrypts the encrypted data using the first and at least second private keys.

12. The method according to claim 11, wherein the smart card is a credit card.

13. The method according to claim 11, wherein the smart card is an identification card.

14. The method according to claim 11, wherein the data is digital information comprises one of computer software, music, literature, audio and/or video information.

15. The method according to claim 11, wherein the public and private keys are asymmetric public and private keys.

16. The method according to claim 15, wherein the asymmetric public keys for the user are obtained from the user.

17. The method according to claim 15, wherein the asymmetric public keys for the user are obtained from a public database.

18. The method according to claim 11, wherein the user authenticates the smart card by entering a personal identification number code.

19. The method according to claim 11, wherein the user authenticates the smart card by entering a biometric identification code.

20. The method according to claim 11, wherein a processor in the smart card decrypts the encrypted data using the private key.

21. A method for controlling the use of data on a device by a user, comprising the steps of:

encrypting data to be sent to the user using at least one public key assigned to the user before distributing the data to the user; and

after distribution of the data to the user, prompting the user to enter at least one private key each time the user wants to use the data, wherein the at least one private key is stored on a smart and the at least one private key is usable but not known by the user and the at least one private key can not be used until the card is activated by

authenticating that the user is authorized to use the smart card, wherein the user inserts the smart card into a smart card reader connected to the device and activates the smart card, wherein the device decrypts the encrypted data using the private key.

22. The method according to claim 21, wherein the smart card is a credit card.

23. The method according to claim 21, wherein the smart card is an identification card.

24. The method according to claim 21, wherein the data is digital information comprises one of computer software, music, literature, audio and/or video information.

25. The method according to claim 21, wherein the at least one public and private keys are asymmetric public and private keys.

26. The method according to claim 25, wherein the at least one asymmetric public key for the user is obtained from the user.

27. The method according to claim 25, wherein the at least one asymmetric public key for the user is obtained from a third party.

28. The method according to claim 21, wherein the user authenticates the smart card by entering a personal identification number code.

29. The method according to claim 21, wherein the user authenticates the smart card by entering a biometric identification code.

30. The method according to claim 21, wherein the user knows all of the private keys except for one private key.

31. The method according to claim 21, wherein a processor in the smart card decrypts the encrypted data using the private key.

32. A method for controlling the use of data on a device by a user, comprising the steps of:

encrypting data to be sold to the user by a seller using at least one public key assigned to the user before distributing the data to the user; and

after distribution of the data to the user, the user is prompted by the device to enter at least one private key each time the user wants to use the data, wherein the at least one private key is stored on a smart and the at least one private key is usable but not known by the user and the at least one private key can not be used until the card is activated by authenticating that the user is authorized to use the smart card, wherein the user inserts the smart card into a smart card reader connected to the device and activates the smart card, wherein the device decrypts the encrypted data using the private key.